Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799

Antonio Villalón Huerta
Grupo S2

Contenidos

- **Introducción.**
  - Problemática de seguridad.
  - ¿Qué es ISO 17799?
  - Historia

- **Estructura de la norma.**
  - Dominios de control.
  - Objetivos de control.

- **Trabajando con ISO 17799.**
  - Auditoría.
  - Consultoría.
  - Implantación.

- **Ventajas.**

- **Conclusiones.**

S2 grupo

Introducción: problemática

- ¿Cómo establecer **qué entendemos por 'seguridad'**?

- Diferentes criterios de **evaluación de la seguridad**: internos a una organización, sectoriales, nacionales, internacionales...

- Multitud de **estándares** aplicables a diferentes niveles:
  - TCSEC (Trusted Computer Security, militar, US, 1985).
  - ITSEC (Information Technology Security, europeo, 1991).
  - Common Criteria (internacional, 1986-1988).
  - *7799 (británico + internacional, 2000).
  - ...

- Actualmente, tras adoptar *7799 como estándar internacional, es el más extendido y aceptado.

S2 grupo

Introducción: ¿qué es ISO 17799?

- ISO 17799 es una norma internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

- ISO 17799 define la **información** como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la **seguridad de la información** es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

- La seguridad de la información se define como la preservación de:
  - **Confidencialidad**. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
  - **Integridad**. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
  - **Disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

S2 grupo

Introducción: ¿qué es ISO 17799?

- El **objetivo** de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

- La adaptación española de la norma se denomina **UNE-ISO/IEC 17799**.

- Se trata de una norma NO CERTIFICABLE, pero que recoge la relación de controles a aplicar (o al menos, a evaluar) para establecer un **Sistema de Gestión de la Seguridad de la Información** (SGSI) según la norma UNE 71502, CERTIFICABLE.

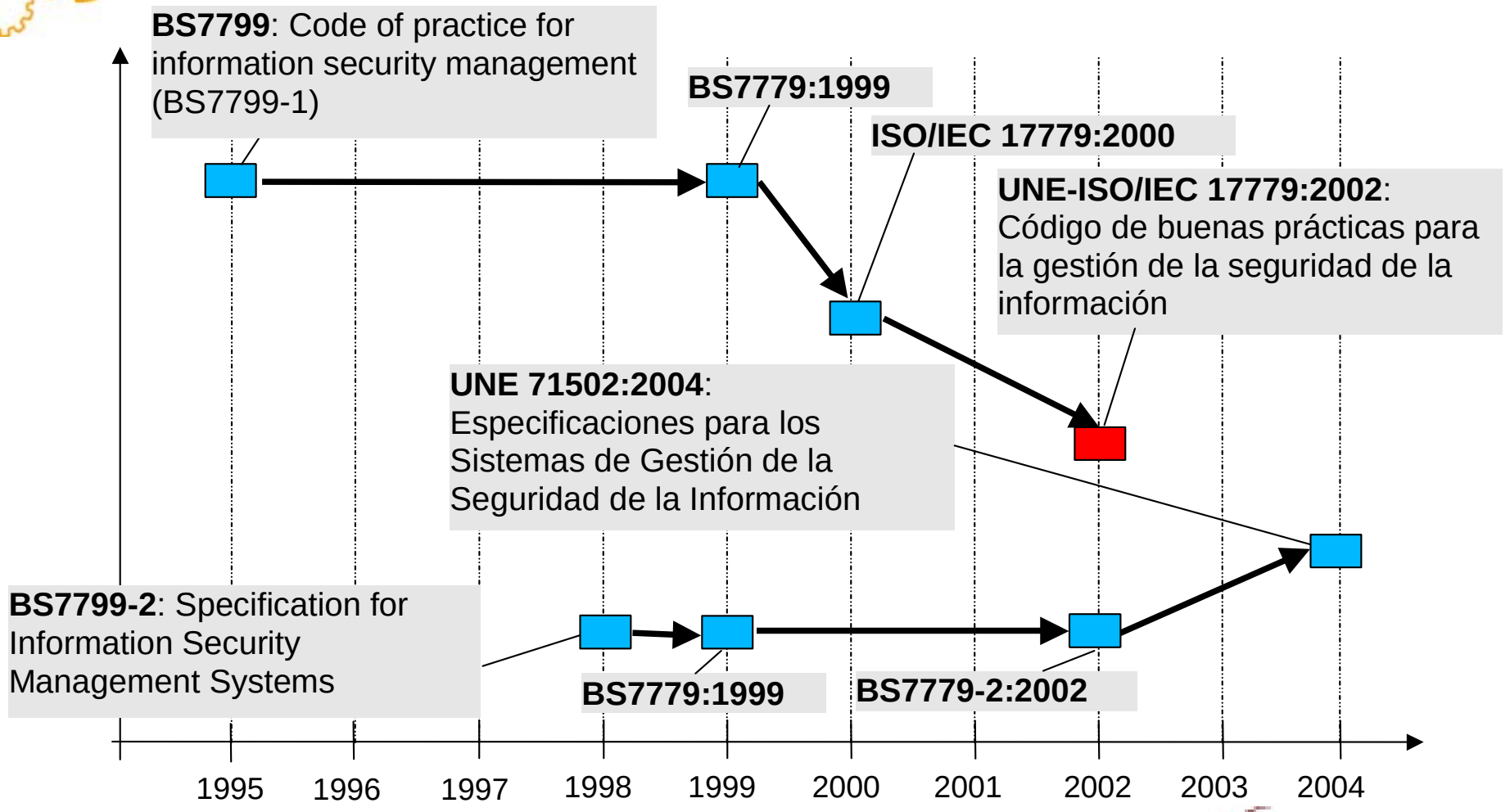
S2 grupo

Introducción: historia

- En 1995 el British Standard Institute publica la norma BS 7799, un código de buenas prácticas para la gestión de la seguridad de la información.
- En 1998, también el BSI publica la norma BS 7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.
- Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:
  - Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
  - Aplicable por toda organización, con independencia de su tamaño.
  - Flexible e independiente de cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la tecnología.
- En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (no existe equivalente ISO).

S2 grupo

Introducción: historia



Estructura: dominios de control

- La norma UNE-ISO/IEC 17799 establece **diez dominios de control** que cubren por completo la Gestión de la Seguridad de la Información:
  1. Política de seguridad.
  2. Aspectos organizativos para la seguridad.
  3. Clasificación y control de activos.
  4. Seguridad ligada al personal.
  5. Seguridad física y del entorno.
  6. Gestión de comunicaciones y operaciones.
  7. Control de accesos.
  8. Desarrollo y mantenimiento de sistemas.
  9. Gestión de continuidad del negocio.
  10. Conformidad con la legislación.
- De estos diez dominios se derivan **36 objetivos de control** (resultados que se esperan alcanzar mediante la implementación de controles) y **127 controles** (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

S2 grupo

Estructura: dominios de control

Estructura: objetivos de control

POLÍTICA DE SEGURIDAD

✓Dirigir y dar soporte a la gestión de la seguridad de la información.

- La alta dirección debe definir una **política** que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad de la información.
- La alta dirección debe **apoyar visiblemente** la seguridad de la información en la compañía.

S2 grupo

Estructura: objetivos de control

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- ✓Gestionar la seguridad de la información dentro de la organización.
- ✓Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.
- ✓Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

- Debe diseñarse una estructura organizativa dentro de la compañía que defina las **responsabilidades** que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma.

- Dicha estructura debe poseer un enfoque **multidisciplinar**: los problemas de seguridad no son exclusivamente técnicos.

Estructura: objetivos de control

CLASIFICACIÓN Y CONTROL DE ACTIVOS

- ✓Mantener una protección adecuada sobre los activos de la organización.
- ✓Asegurar un nivel de protección adecuado a los activos de información.

- Debe definirse una **clasificación** de los activos relacionados con los sistemas de información, manteniendo un **inventario** actualizado que registre estos datos, y proporcionando a cada activo el nivel de **protección** adecuado a su criticidad en la organización.

S2 grupo

Estructura: objetivos de control

SEGURIDAD LIGADA AL PERSONAL

- ✓Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.
- ✓Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
- ✓Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Estructura: objetivos de control

SEGURIDAD LIGADA AL PERSONAL (II)

- Las implicaciones del **factor humano** en la seguridad de la información son muy elevadas.
- Todo el personal, tanto **interno** como **externo** a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
- Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc.
- Procesos de **notificación de incidencias** claros, ágiles y conocidos por todos.

Estructura: objetivos de control

SEGURIDAD FÍSICA Y DEL ENTORNO

- ✓Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
- ✓Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- ✓Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

- Las áreas de trabajo de la organización y sus activos deben ser clasificadas y **protegidas** en función de su criticidad, siempre de una **forma adecuada** y frente a cualquier **riesgo factible** de índole física (robo, inundación, incendio...).

S2 grupo

Estructura: objetivos de control

GESTIÓN DE COMUNICACIONES Y OPERACIONES

- ✓Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- ✓Minimizar el riesgo de fallos en los sistemas.
- ✓Proteger la integridad del software y de la información.
- ✓Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- ✓Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- ✓Evitar daños a los activos e interrupciones de actividades de la organización.
- ✓Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

- Se debe garantizar la seguridad de las **comunicaciones** y de la **operación** de los sistemas críticos para el negocio.

Estructura: objetivos de control

CONTROL DE ACCESOS

- ✓Controlar los accesos a la información.
- ✓Evitar accesos no autorizados a los sistemas de información.
- ✓Evitar el acceso de usuarios no autorizados.
- ✓Protección de los servicios en red.
- ✓Evitar accesos no autorizados a ordenadores.
- ✓Evitar el acceso no autorizado a la información contenida en los sistemas.
- ✓Detectar actividades no autorizadas.
- ✓Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

- Se deben establecer los **controles de acceso adecuados** para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

S2 grupo

Estructura: objetivos de control

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- ✓Asegurar que la seguridad está incluida dentro de los sistemas de información.
- ✓Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- ✓Proteger la confidencialidad, autenticidad e integridad de la información.
- ✓Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura.
- ✓Mantener la seguridad del software y la información de la aplicación del sistema.

- Debe contemplarse la seguridad de la información en **todas las etapas** del ciclo de vida del software en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento...

Estructura: objetivos de control

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

✓Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.

- Todas las situaciones que puedan provocar la **interrupción** de las actividades del negocio deben ser **prevenidas** y **contrarrestadas** mediante los planes de contingencia adecuados.
- Los **planes de contingencia** deben ser probados y revisados periódicamente.
- Se deben definir **equipos de recuperación** ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

S2 grupo

Estructura: objetivos de control

CONFORMIDAD

- ✓Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.
- ✓Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.
- ✓Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

- Se debe identificar convenientemente la **legislación aplicable** a los sistemas de información corporativos (en nuestro caso, LOPD, LPI, LSSI...), integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.

- Se debe definir un plan de **auditoría interna** y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

S2 grupo

Auditoría

- ¿Somos seguros? ¿**Muy** seguros? ¿**Poco** seguros? ¿**Relativamente** seguros?...

- Trabajo de **auditoría ISO 17799**: valoración del nivel de adecuación, implantación y gestión de cada control de la norma en la organización:
  - Seguridad lógica.
  - Seguridad física.
  - Seguridad organizativa.
  - Seguridad legal.

- Referencia de la seguridad de la información **estándar** y aceptada internacionalmente.

- Una vez conocemos el estado actual de la seguridad de la información en la organización, podemos **planificar** correctamente su mejora o su mantenimiento.

Auditoría

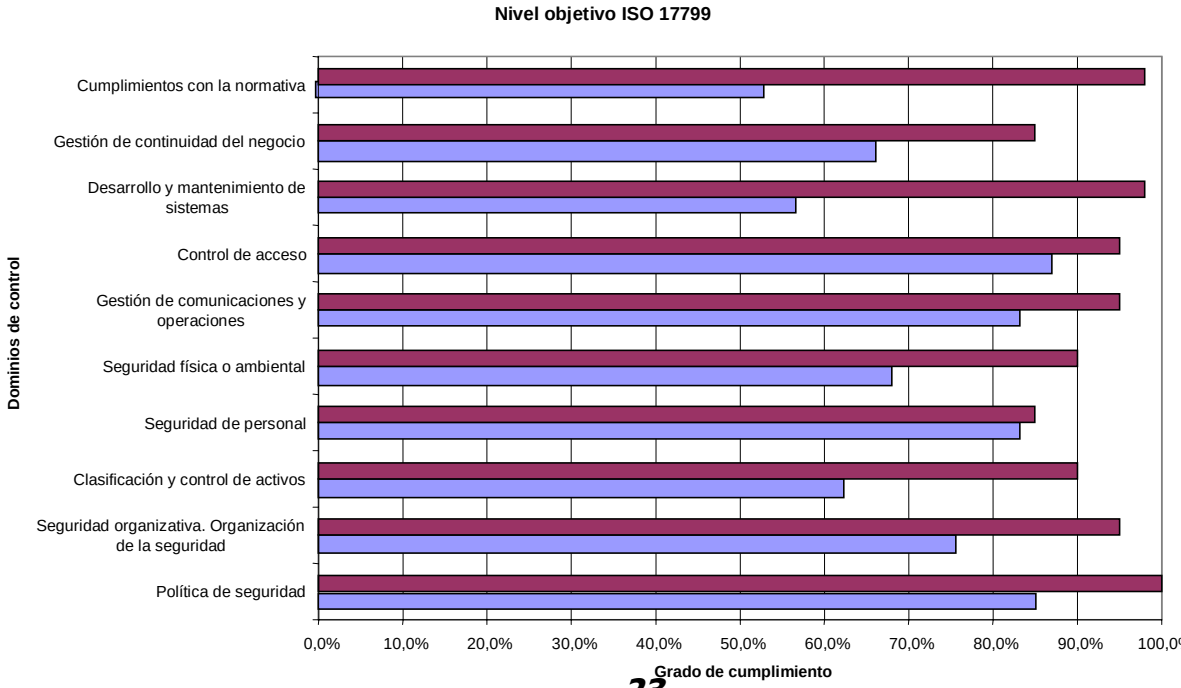
- Una auditoría ISO 17799 proporciona **información precisa** acerca del **nivel de cumplimiento** de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.

1	1			Información sobre la política de seguridad			100%	1,6%	
		1		Documento de política de seguridad			80%	1,3%	Nulo
		2		Revisión y evaluación			20%	0,3%	Nulo
2	3	10	*Seguridad organizativa. Organización de la seguridad*		7,9%				
				Infraestructura de la Seguridad de la Información.		60%		4,7%	
	1	1		Foro de gestión de seguridad			20%	0,9%	Nulo
		2		Coordinación de la seguridad de la información.			10%	0,5%	Nulo
		3		Asigancián de responsabilidades en material de seguridad de la información			15%	0,7%	Nulo
		4		Proceso de autorización para instalaciones de proceso de información			20%	0,9%	Muy Bajo
		5		Asesoramiento especializado en materia de seguridad			15%	0,7%	Nulo
		6		Cooperación entre organizaciones			10%	0,5%	Nulo
		7		Revisión independiente de la seguridad de la información			10%	0,5%	Nulo
	2			Seguridad frente al acceso por parte de terceros.		20%			
		1		Identificación de riegos del acceso de terceras partes.			40%	0,6%	Muy Bajo
		2		Requerimientos de seguridad en contratos con terceross			60%	0,9%	Nulo
	3			Externalización. Outsourcing.		20%			
		1		Requerimientos de seguridad en la subcontratación de servicios.			100%	1,6%	Nulo
3	2	3	*Clasificación y control de activos*		2,4%				
	1			Responsabilidades en los activos.		60%			
		1		Inventario de activos			100%	1,4%	Muy Bajo
	2			Clasificación de la información		40%			
		1		Pautas de clasificación			70%	0,7%	Nulo
		2		Rotulado y manejo de la información			30%	0,3%	Nulo
4	3	10	*Seguridad de personal*		7,9%				
				Seguridad en la definición de puestos de trabajo y la asignación de recursos.		40%			
	1	1		Inclusión de responsabilidades de seguridad en el puesto de trabajo.			40%	1,3%	Nulo
		2		Selección y política de personal			20%	0,6%	Nulo
		3		Acuerdos de confidecrialidad			20%	0,6%	Nulo
		4		Términos y condiciones de empleo			20%	0,6%	Nulo
	2			Entrenamiento de los usuarios.		30%			
		1		Formación y educación en material de seguridad			100%	2,4%	Nulo
				Respuesta ante incidentes y anomalías en materia de seguridad		30%			

S2 grupo

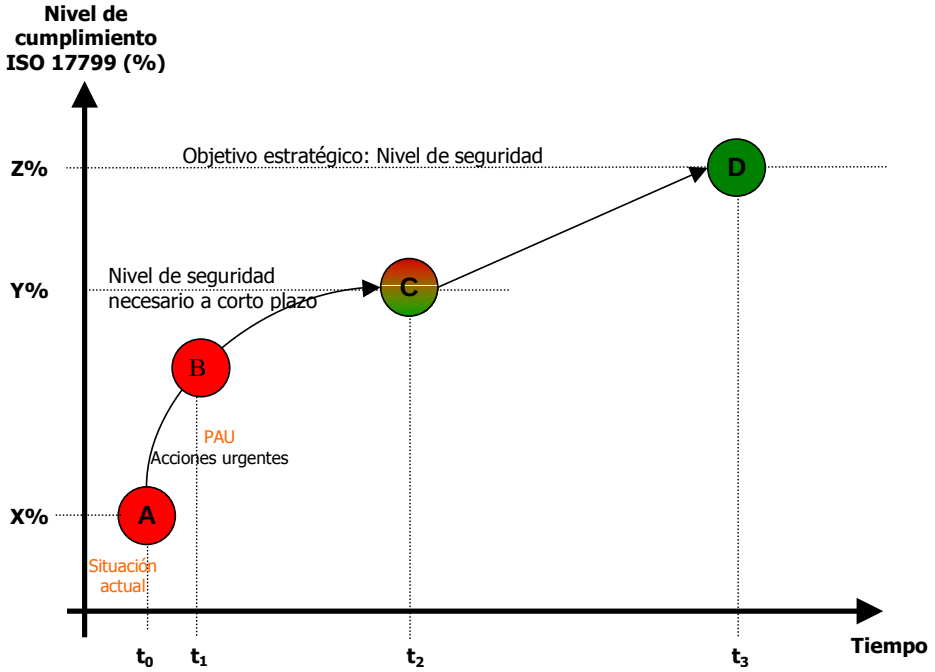
Consultoría

- Conociendo el nivel de cumplimiento actual, es posible determinar el nivel mínimo aceptable y el nivel objetivo en la organización:
  - Nivel **mínimo aceptable**. Estado con las mínimas garantías de seguridad necesarias para trabajar con la información corporativa.
  - Nivel **objetivo**. Estado de seguridad de referencia para la organización, con un alto grado de cumplimiento ISO 17799.



Consultoría

- A partir del nivel mínimo aceptable y el nivel objetivo, podemos definir un plan de trabajo para alcanzar ambos a partir del estado actual.
  - Nivel **mínimo aceptable**. Implantación de los controles **técnicos** más **urgentes**, a muy **corto plazo**.
  - Nivel **objetivo**. Se desarrolla en el tiempo dentro del **Plan Director de Seguridad** corporativo, y es el paso previo a la **certificación UNE 71502**.



Implantación

- ISO 17799 **no** es una norma tecnológica.
  - Ha sido redactada de forma flexible e independiente de cualquier solución de seguridad específica.
  - Proporciona buenas prácticas neutrales con respecto a la tecnología y a las soluciones disponibles en el mercado.

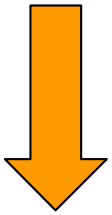
- Estas características posibilitan su implantación en todo tipo de organizaciones, sin importar su tamaño o sector de negocio, pero al mismo tiempo son un argumento para los detractores de la norma.

- ¿Cómo traducir especificaciones de alto nivel a soluciones concretas, para poder implantar ISO 17799?
  - Trabajo de consultoría, interna o externa.

S2 grupo

Implantación: un ejemplo

- **Dominio de control:** Gestión de comunicaciones y operaciones
  - **Objetivo de control:** proteger la integridad del software y de la información.
    - **Control:** Controles contra software malicioso.
- *"Se deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concienciar a los usuarios".*



Consultoría

- Normativa de uso de software: definición y publicitación en la Intranet.
- Filtrado de contenidos: X - Content Filtering v3.4.
- Antivirus de correo: Y – Antivirus v2.0.
- Antivirus personal: Z - Antivirus v4.5.

S2 grupo

Ventajas de la norma

- La adopción de la norma ISO 17799 proporciona **diferentes ventajas** a cualquier organización:

  - Aumento de la **seguridad efectiva** de los sistemas de información.
  - Correcta **planificación** y gestión de la seguridad.
  - Garantías de **continuidad del negocio**.
  - **Mejora contínua** a través del proceso de auditoría interna.
  - Incremento de los niveles de **confianza** de nuestros clientes y *partners*.
  - Aumento del **valor comercial** y mejora de la **imagen** de la organización.
  - ...
  - **¡CERTIFICACIÓN!** (UNE 71502)

S2 grupo

Conclusiones

- ISO 17799 es una norma internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información, adoptada en España como norma UNE-ISO/IEC 17799.

- La norma se estructura en **diez dominios de control** que cubren por completo todos los aspectos relativos a la seguridad de la información.

- Implantar ISO 17799 requiere de un trabajo de **consultoría** que adapte los requerimientos de la norma a las necesidades de cada organización concreta.

- La adopción de ISO 17799 presenta diferentes **ventajas** para la organización, entre ellas el primer paso para la **certificación** según UNE 71502.

Ni la adopción de ISO 17799, ni la certificación UNE 71502, ni... garantizan la inmunidad de la organización frente a problemas de seguridad.

S2 grupo


30 SEPTIEMBRE 2004 VALENCIA
El Sistema de Gestión de Seguridad de la Información
"La nueva norma UNE 71502"